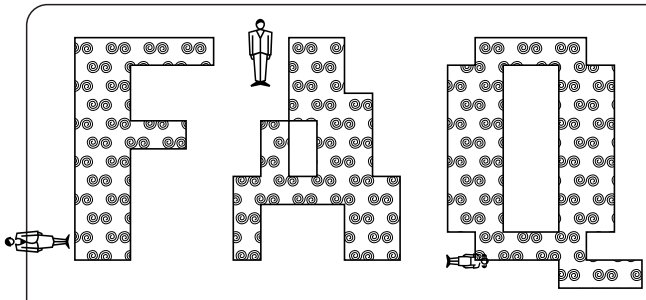


Frequently Asked Question

いまさら聞けない

いまだから聞きたい

このコーナーでは読者の皆さんのインターネットに関する疑問や質問にお答えします。「？」と感じたことはどのようなことでも構いませんので、下記のメールアドレスまでご質問ください。なお、ご質問へのメールでの回答はできませんのでご了承ください。

○ご質問はこちらまで
im-faq@impress.co.jp

今月のポイント

1 無線LANで使うRADIUSサーバーとは？

2 時刻認証は何を認証するのか？

Q

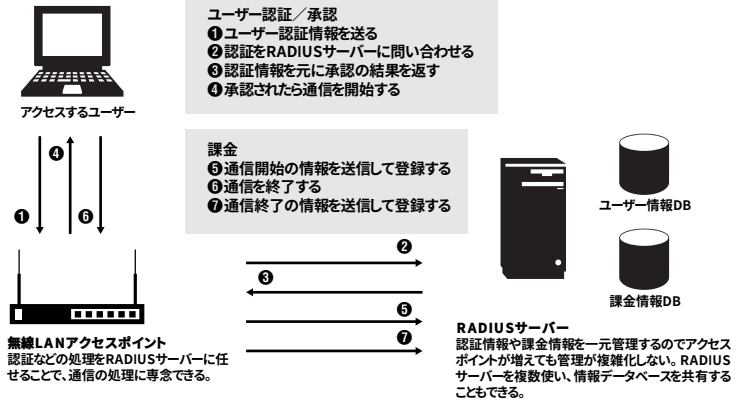
無線LANのセキュリティーでRADIUSサーバーを使うと聞きました。RADIUSという名前は以前に聞いたことがありますが、どんな仕組みで無線LANのセキュリティーが守られるのでしょうか？（富山県　Kさん）

A

RADIUSは「Remote Authentication Dial-In User Service」の略で、リモートアクセスでのユーザー認証を一元化する仕組みです。ダイアルアップ接続でネットワーク上のコンピュータを使う場合の認証のために、リビングストーン社（現在のルーセント・テクノロジーズ社）が開発したもので、IETFで標準化されています。RADIUSサーバーはネットワークサービス利用者のユーザー名やパスワードなどをまとめて管理して、RADIUSクライアント（VPNサーバー、リモートアクセスサーバーなどのネットワーク機器）へのアクセスに対する認証、承認、課金の処理を集中的に行います。現在でもISPではこの機能を利用してユーザーの認証や課金を行っています。認証をネットワーク機器自身ではなくRADIUSサーバーに行わせることで、ユーザー数を増やすなどの管理が楽になります。また、さまざまな認証方式に対応しているのも特徴です。

無線LANのアクセスポイントに、認証に特化したRADIUSサーバーの仕組みを組み込むことで、機器の性能を落とすことなくセキュリティーを確保することができます。家庭で無線LANを使う場合にはアクセスポイントの持つ認証で問題ありませんが、企業などで無線LANを使う場合にはRADIUSが有効でしょう。（鈴木雅登）

RADIUSサーバーによる認証／課金の仕組み



多数の無線LANアクセスポイントのリモートアクセスの情報を一元管理

Q

「時刻認証」というものがあると聞きました。どういう仕組みで「時刻」を認証するのでしょうか？
（東京都　晃一さん）

A

「この時刻」に「この内容」で存在した認証
電子政府や電子取引に向けて本格的に普及か

時刻認証は、電子データが「ある特定の時間に存在していた」ことと同時に「ある特定の時間以降改ざんされていない」ことを証明するための仕組みです。簡単に言えば、紙の情報と同じ信頼性を電子でも実現可能にした仕組みということです。

たとえば電子メールでは「50万円を○○口座に振り込んで」と書かれていても、メール転送の中間地点で金額や送金先を書き換えられます。電子データは、紙に比べて流通は非常に便利なのですが、修正や改ざんが容易という脆弱性があります。改ざんの痕跡すら残さないという問題や情報の原本と複製の識別も困難なことから、オリジナルの権利の主張も難しくなります。そこで、電子データの信頼性を高めるために考え出された仕組みが時刻認証サービスなのです。

時刻認証サービスには、信頼できる時刻の配信・監査を行うサービスと電子データの存在日時を特定するタイムスタンプサービスの2種類があります。ここでは、利用者にとって最も身近なタイムスタンプサービスについて説明します。

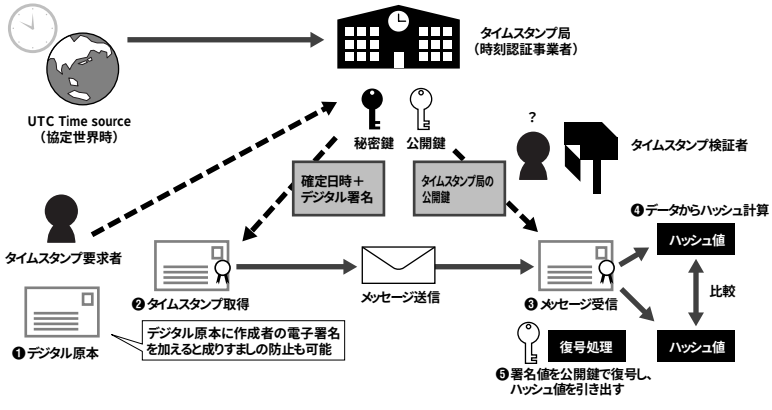
タイムスタンプサービスは、対象となる電子データに第三者機関が時刻情報を加えて電子署名する仕組みです。これにより、電子データの改ざんが困難になると同時にその電子データが存在した日時を特定できるのです。インターネットを利用した電子的な契約、証券取引、カルテ、特許申請、オークション入札など、さまざまな電子取引で利用されると予想されています。

タイムスタンプには、暗号技術とハッシュ（後述）関数を応用した「電子署名」が使われます。電子データから一意な「ハッシュ値」を生成してこれに時刻情報を加えたものを、認証事業者の秘密鍵で暗号化したものがタイムスタンプとなります。タイムスタンプを認証局の公開鍵で復号できれば電子署名が確認できます。また、取り出したハッシュ値と現在のデータのハッシュ値が同じ値であれば、電子データが改ざんされていないことが確認できます。ハッシュ値とは、電子データの指紋のようなデータで、1ビットでも変更されるとまったく異なったハッシュ値になります。

タイムスタンプに使われる「時刻」の信頼性も大切です。コンピュータの内部で使われている時刻はだれでも修正できるうえに精度も低いものです。実際にタイムスタンプサービスを行っているアマノやセイコーインスツルメンツでは、「時刻認証局」という信頼できる機関から配信された、協定世界時（UTC）と同期した正確な時刻を使用します。

電子データの原本性保証を高めるタイムスタンプや時刻認証サービスは、これから本格化するでしょう。　（井上正和）

時刻認証の仕組み



タイムスタンプが付けられたPDFファイルの例

時刻認証されたPDFファイルのタイムスタンプをダブルクリックするとプラグインがタイムスタンプを検証してくれる。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp